HEADQUARTERS, DEPARTMENT OF ENERGY

COMPUTER PROTECTION PLAN (CPP)

for

UNCLASSIFIED SYSTEMS

PART I

HEADQUARTERS COMPUTER PROTECTION PLAN

June 1998

CPPM Approval ___________________________________

U.S. DEPARTMENT OF ENERGY

Assistant Secretary for Human Resources and Administration
Office of the Chief Information Officer
Office of Information Management

CONTENTS

ENCLOSURES:

PART II

PART I

1. PROGRAM OVERVIEW

1.1 Authority

The Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*, and the Department of Energy (DOE) Order 1360.2B, *Unclassified Computer Security Program*, establish requirements for the protection of sensitive and mission-essential information collected, processed, transmitted, stored, or disseminated in general support systems and major applications. OMB A-130, Appendix III, requires that security controls be established for all general support systems under the presumption that all information systems (IS) contain some sensitive information. DOE 1360.2B requires that all unclassified ISs have a plan for protecting information, and that mission-essential applications be included in contingency planning.

1.2 Purpose

The Headquarters DOE *Computer Protection Plan (Plan) for Unclassified Systems* is issued by the DOE Headquarters Computer Protection Program Manager (CPPM) to assist DOE Headquarters organizations in complying with computer security requirements, and managing systems covered by DOE 1360.2B. This Plan, and the National Institute of Standards and Technology (NIST), *User Guide for Developing and Evaluating Security Plans for Unclassified Federal Automated Information Systems* (see Appendix "A"), establish minimum security controls, that when implemented, will provide protection for ISs as required by OMB Circular A-130. They give sufficient guidance for DOE Headquarters organizations to successfully implement the unclassified computer security program. This Plan and the NIST Guide provide controls, methods, techniques, outlines, and formats that can be used to protect DOE Headquarters unclassified computer systems, major applications, and their information.

The NIST Computer Security Resource Clearinghouse contains recent publications from a variety of sources that deal with information security issues, and may be accessed at *http://csrc.ncsl.nist.gov/*, under Publications.

1.3 Scope

To meet the requirements of the DOE 1360.2B, a Computer Protection Program Manager (CPPM) is appointed for each DOE and contractor site. The CPPM for Headquarters resides in the Human Resource and Administrations's Office of Information Management (HROIM). The CPPM is responsible for establishing, implementing, and administering a management control process that safeguards unclassified computer systems and mission-essential applications. The CPPM must also prepare a Headquarters Plan, and review it on an annual basis. The CPPM relies on each organization to appoint an Assistant Computer Protection Program Manager (ACPPMs) to assist in compliance.

This Plan provides information for DOE Headquarters organizations and supporting contractors that own, manage, or support DOE unclassified IS as required by law and/or contract. The Plan and enclosures, NIST Guide, and referenced documents constitute the guidance for the Headquarters Unclassified Computer Security Program. The Plan and NIST Guide contain the information necessary for ACPPMs to assist the CPPM in carrying out an effective Headquarters computer security program.

The DOE Order 471.2, *Information Security Program*, dated 09-26-95, and the accompanying Manual, address classified systems and applications that are outside the scope of this document.

This Plan consists of two parts. Part I is for use by the CPPM and ACPPMs and consists of the following chapters.

- Chapter 1. Contains an overview of the program.
- Chapter 2. Contains a synopsis of the program management methodology and describes procedures for computer security reviews, certification, and approval for processing.
- Chapter 3. Specifies responsibilities of organizations and designated individuals.
- Chapter 4. Provides information to help in identifying systems requiring protection.
- Chapter 5. Details the minimum security controls for Headquarters unclassified systems.
- Chapter 6. Discusses the Computer Security and Privacy Plan (CSPP)
- Chapter 7. Explains the risk assessment and management process.
- Chapter 8. Addresses continency planning.
- Chapter 9. Outlines the computer security training program.
- Enclosures. Provide tools to assist ACPPMs in the implementation of their computer security programs.
- Appendix A. Contains the NIST *User Guide for Developing and Evaluating Security Plans for Unclassified Federal Automated Information Systems*.

The Plan, Part II, contains individual organizational Computer Security and Privacy Plans (CSPPs) and is for use by the CPPM for program management and oversight.

1.4 Applicability

This Plan applies to organizational computer systems and major applications processing unclassified information at DOE Headquarters. The exceptions are the Energy Information Administration and the Office of Civilian Radioactive Waste Management. Systems accredited for classified processing while processing in an unclassified mode (periods processing), must also conform to the controls defined in their respective Classified IS Security Plans.

2. PROGRAM MANAGEMENT SYNOPSIS

2.1 Headquarters Management Control Process

The Headquarters Management Control Process is composed of two distinct components; a set of objectives, and a concept of implementation. The objectives, when accomplished, provide the foundation for a viable unclassified computer security program. The methods of implementation will ensure the program is effectively realized.

2.2.1 Objectives of the Management Control Process

This Plan is intended to accomplish several major objectives.

- Document the administrative process for implementing the unclassified computer security program.

- Identify unclassified computer systems and major applications within DOE Headquarters that require protection.

- Establish minimum security requirements for unclassified computer systems and major applications.

- Provide additional guidance, standards, assistance, training, and new technology to ensure their protection.

- Establish additional controls to enhance the security of applications identified to have an added degree of sensitivity or vulnerability of a particular concern.

- Provide information to aid in the development of Computer Security and Privacy Plans (CSPPs) for documenting conformance with Headquarters policy and procedures.

- Establish oversight procedures for evaluating the effectiveness of existing measures implemented to provide protection to systems processing unclassified information.

- Require organizations to establish user rules of acceptable use and behavior for organizational-sponsored systems, and the sanctions users should expect for not following these rules.

2.2.2 Concept of the Management Control Process

There are several major elements involved in the concept for a management control process of this program. A brief synopsis follows.

- **Responsibility**. The CPPM has the overall responsibility for the Headquarters unclassified computer security program. The CPPM coordinates a network of appointed ACPPMs from

Headquarters organizations to help conduct the program and maintain their respective CSPPs. (See Chapter 3)

- **System and Information Identification**. Each organization is responsible for identifying unclassified computer systems and major applications under their cognizance. They are also responsible for identifying information having an added degree of sensitivity that requires additional protective measures. (See Chapter 4)

- **Security Requirements**. This Plan specifies the minimum security requirements and safeguards for protection of unclassified computer systems, applications, and the information contained therein. (See Chapter 5)

- **Documentation**. This Plan and individual CSPPs document the security process. Organizations develop CSPPs for unclassified computer systems (excluding personal computers) and major applications under their cognizance. CSPPs are prepared by the ACPPM to certify that security controls are in place, and approved by the Program Manager. Copies are forwarded to the CPPM and become attachments to this Plan in Part II. This Plan and attachments are used as the basis for the Headquarters Computer Security Program. (See Chapter 6 and Enclosure (C).)

- **Security Certification and Approval of Unclassified General Support Computer Systems**. Section 2.4.1 outlines the security certification and approval process for unclassified general support computer systems.

- **Security Certification and Approval of Unclassified Major Applications**. Section 2.4.2 outlines the security certification and approval process for major applications.

- **Program Oversight**. Activities are performed at various levels within Headquarters to provide oversight of the program. CPPM review of security program effectiveness will be an ongoing process and adjustments to procedures outlined in this Plan will be made as necessary. (See section 2.5)

- **Incident Handling**. Section 2.8 describes the procedures and measures for responding to security incidents and the reporting of findings.

- **Training**. The CPPM has established basic security training requirements for ACPPMs and users that comply with the Computer Security Act. Actual user training is the responsibility of the organization. ACPPMs attend CPPM-sponsored training and, in turn, ensure that their users receive computer security training prior to accessing Headquarters systems. Any specialized training required for maintenance and computer support personnel is the responsibility of the cognizant official (e.g., Program Manager, application owner, ACPPM). (See Chapter 9)

2.3 Computer System Operational Environments

To simplify defining security features common to like computer systems, operating environments are addressed based on their operational structure. Headquarters IS may be either standalone or networked systems. Systems may consist of a host processor, nodes, paths and operating system and applications software.

2.3.1 Standalone Computer System

Standalone computer systems are also referred to as desktop systems, microcomputers, personal computers (PCs), workstations, or Headquarters Automated Office Support Systems (AOSS). AOSS is a generic DOE term which typically applies to single user workstations. These systems are located throughout Headquarters and are used primarily for word processing, database management, spreadsheet production, and graphics. A microprocessor may also be a piece of test equipment. The controls for this type of system environment are found in section 5.4.2. A specific system CSPP is not required.

2.3.2 Host Computer

A host computer is a computer that supports the function of maintaining diversified applications, functions and/or networking. It is typically a large mainframe computer. It can also be a local area network with centrally loaded, shared and controlled software. This is where the operating software is based that requires a degree of physical protection from unauthorized access and inadvertent destruction.

2.3.3 Networked Computer System

Network systems consist of a group of terminals and computer processors that are linked directly to a host computer or to servers through communications paths and nodes. These processors may be microprocessors, minicomputers, mainframe computers, or other systems. The network computer system also includes the software applications and information that reside on them (e.g., bulletin board systems, home pages, shared COTS software.)

A networked system is considered a general support computer system and requires that a CSPP be developed and maintained that describes the protection features. The CPPM is available to review and comment on the CSPP. Formal system security certification (acceptance and approval to operate) will be performed by a Program Manager. A single CSPP may be developed for similar systems under the same management authority, with attached sheets noting any unique system specific characteristics.

2.3.3.1 Node

A computer system node may be a PC, mainframe processor, server, printer, router, gateway or any other hardware component that is addressable and connected in a network configuration.

2.3.3.2 Path

A path is the route that the information travels after the processing state and during transmission. The path may be a trusted path, as in a predetermined protected distribution system, or random and open to the public, as on the Internet. The latter may have varying degrees of protection from none, to high (i.e., information encryption).

2.3.4 Software

Software relates to the programs that issue instructions to control the processing. They may be acquired with the host platform, locally developed, copied from another system, or commercially procured.

2.3.4.1 Application Software

For the purpose of this Plan, computer applications consist of the software and the information that the application processes. All Federal applications require some level of protection. An application that requires special attention to security due to the risk and magnitude of the harm that could result from the loss, misuse, or unauthorized access to, or modification of the information, is considered to be a major application (major is synonymous with mission-essential). A major application requires that a CSPP be developed and that security certification be issued by the ACPPM. Formal approval to operate will be granted by a Program Manager prior to processing.

2.3.4.2 Operating System

An operating system is a program that controls a computer and makes it possible for users to enter and run their own programs. Operating systems perform basic tasks such as keeping track of files and directories on the disk, controlling peripheral devices such as disk drives and printers, recognizing input from the keyboard, and sending output to the display screen. The operating system may typically be responsible for security, making sure that unauthorized users do not access the system. Protection of the operating system from unauthorized access is the most important consideration in system security.

2.3.4.3 Commercial Off-the-Shelf Software (COTS)

COTS relates to any prepackaged commercial software that is procured to either perform a specific function, or support a function that is already planned or in place. Source code is normally unavailable for this type of software, and any assurances are gained from manufacturers product warranty, reputation, or independent testing.

2.4 Unclassified General Support Systems and Major Applications Assurance

General support computer systems and major applications that process or store unclassified information must obtain Headquarters security certification and Program Manager approval to begin operational processing. For the purpose of this Plan, the term "computer system" is synonymous with the "general support system" as described in OMB A-130.

2.4.1 Unclassified Computer Systems Approval and Certification

With the revision of this Plan, the responsibilities for certification and approval of computer systems have been decentralized and delegated to organizational ACPPMs and Program Managers. Computer systems developed and hardware selected will incorporate the minimum computer security features outlined in this Plan and/or the NIST Guide. To support this effort, the ACPPM will review system requirements documents and make recommendations on computer security related issues. The ACPPM will also review system documentation, plans, and tests, and issue a formal statement of security certification. The Program Manager for the functional area that the system supports will issue an approval for the system to begin or continue processing based on the risk as indicated in the security certification and supporting documentation.

Enclosure (A), Computer System Security Certification and Approval Checklist, outlines the certification and approval process.

2.4.2 Major Application Approval and Security Certification

An IS software application is considered major if it is critical to the Department or organization mission (mission-essential); involves high development, operating or maintenance costs; and if the risk and magnitude of harm that could be experienced from the loss, misuse, unauthorized access to or modification of the information would have an adverse impact on the Department's ability to perform their missions.

All proposed applications identified as major and/or mission-essential are to be designed in accordance with the DOE Guide 200.1-1, *Software Engineering Methodology* (SEM), or local equivalent. They should follow the security processes as prescribed in the SEM, support the documented security objectives and security controls included in this Plan, and have security certification obtained confirming that required security measures are in place and functional.

The ACPPM will review design and test documentation for applications that will process unclassified information. Applications determined to be mission-essential will be listed in the CSPP for the host system on which the application resides, wherein the data files and application program are referred to synonymously and collectively as the system. It must also be incorporated into the Headquarters Administrative Computer Center's Continuity of Operations Plan.

The two primary means of assuring that applications processing unclassified information support minimum established DOE security requirements are; 1) initial security certification, and; 2) security recertification. To maximize security assurance of an application, security issues must be addressed at inception, through development and implementation, during maintenance, and upon system retirement.

DOE Headquarters software applications developed under the HROIM oversight are certified when Enclosure (A), DOE Headquarters General Support System/Major Application Security Certification and Approval Checklist, is completed or a comparable acceptance/certification statement is contained in the final acceptance document. This checklist is prepared and certified by the ACPPM, and formally approved by the Program Manager. These documents are retained as part of the development documents held by the system/application owner.

The certification process is not applicable to commercial-off-the-shelf software (COTS) if the software will be implemented Headquarter-wide. COTS procurements will be approved by the Program Manager prior to installation.

2.4.2.1 Initial Certification

When a new or existing application will access, process, or store unclassified information, security measures must be incorporated to ensure adequate protection of information. The ACPPM security review will run in conjunction with the application development and acceptance process. The SEM identifies the phases of development where security has an impact. Security features will be included in the design document at the appropriate stages as outlined in the SEM. The ACPPM reviews and provides security related comments to the project manager on the design document. The final documentation, to include test results and Enclosure (A), are reviewed by the ACPPM for formal comment. A copy of Enclosure (A) is to be filed with the CSPP. Developments external to HROIM are to follow a similar process. The ACPPM certifies the application for Plan conformance and a Program Manager gives formal approval to run the application operationally.

2.4.2.2 Previous Certification or Recertification

Systems and applications need to be recertified every three years, or when the system/application undergoes mandatory modifications or enhancements, whichever comes sooner. The ACPPM reviews requirements and certifies that security requirements are in place and effective by completing and signing the certification checklist. The Program Manager will provide approval to continue processing.

When an application has been previously certified or recertified, documentation must indicate that the application was certified within the last three years and that application characteristics have not changed significantly. The application must be included in a CSPP with a copy submitted to the CPPM for information and review. The recertification process includes a review of application and system security documentation. It also necessitates a complete examination of security safeguards and procedures used to ensure that DOE security requirements are being satisfied.

2.5 Computer Security Review Process

Security reviews will be conducted on all Headquarters systems processing, storing, or accessing unclassified information. The review process currently consists of security reviews by external agents (General Accounting Office, OMB, NIST), by internal Headquarters reviewing elements (Environmental Safety and Health (EH), Inspector General (IG)), and by the CPPM and the ACPPM.

2.5.1 Internal DOE Reviews

Internal DOE Computer Security Program reviews may be conducted at irregular intervals and can be motivated by known or unknown conditions. The offices of EH and the IG conducts internal reviews. The process involves a review of the effectiveness of the unclassified computer security program. The reviews focus primarily on program management, but may scrutinize selected systems and users, as determined by the reviewers.

As resources permit, the CPPM schedules and conducts security reviews of organizations to ensure that computer security features and measures outlined in this document and CSPPs are implemented. These reviews also ensure that applicable systems and their data are being reasonably protected. The CPPM may also evaluate aspects of the CSPPs through live testing, mock intrusion, scenarios, events, etc. The review process assesses DOE and Headquarters security directives compliance.

Random security reviews of individual systems, however, are the responsibility of the ACPPM. The review includes compliance and system audits on unclassified systems and a review of system Continuity of Operations Plans (COOP). A random sampling of personal computers will be conducted as defined in the organizational computer security policy. The performance and the results of each security review will be documented and retained by the ACPPM for three years.

Enclosures (B), Self Assessment Guidelines, and Enclosure (D), Continuity of Operations Plan Emergency Readiness Evaluation Questionnaire, are provided to assist in conducting these reviews.

2.6 Risk Management

An informal risk management process is performed, from a facility perspective, to examine the security safeguards in place, identify the threat(s) to the system(s), and document the vulnerability of the system(s) to the threat(s). The process helps determine if further safeguards are required for the facility and native system(s) or if the risk of operation is acceptable. The ACPPM is responsible for ensuring that the risk management process is accomplished and maintained on each facility housing unclassified systems (except PCs) within their organization. (See section 5.4.1.7)

2.7 Continuity of Operations Planning

Organizations are responsible for planning continuity of operations in the event of unavailability of the system/application to the Department. Individual application owners are responsible for determining the mission-essentialness of the data being processed by their application and for determining the potential impact of losing the capability to process that data. If the application processes mission-essential data, the application owner addresses contingency planning and notifies the appropriate computer processing installation. Recovery priority is determined and documented in the disaster recovery plan for the facility, as agreed upon by the application owner and the IS facility manager.

2.7.1 Disaster Recovery Plans

System managers are responsible for determining the potential impact of the loss of the installation housing IS and applications that perform mission-essential processing. If the installation is determined to be mission-essential, a disaster recovery plan is formulated.

2.7.2 Contingency Plans

The application owners are responsible for the contingency planning of their specific applications to ensure a means of alternate processing during the loss of primary processing support.

2.8 Computer Security Incident Handling

Computer security incidents must be reported to the ACPPM, and be investigated by either the ACPPM or the ACPPM's agent. Depending on the nature of the incident, it should also be reported to the CPPM, and if warranted, the cognizant Headquarters Security Officer. Reporting computer incidents to the CPPM allows analysis of the incident for the sharing of common vulnerability and threat information to all Headquarters ACPPMs.

2.8.1 Incident Category

A computer security incident is the occurrence of an event that has, or could, adversely affect normal secure computer operations. Examples of major incidents are unauthorized access, theft, fire or water damage, a natural disaster, circumvention of safeguarding controls, or the discovery of vulnerability. An example of a minor incident is the identification of a localized computer virus, malicious code, or the introduction of unauthorized software programs, software bugs or a power failure.

A significant computer security incident is the occurrence of an IS-related event that would be of concern to senior DOE management due to its affect on DOE missions, potential for public interest, embarrassment to the organization, or the possibility of its transference to another facility.

2.8.2 Documenting Reported Incidents

All incidents are to be reported to the ACPPM. The ACPPM will investigate incidents, and if warranted, report them to the CPPM. Significant computer security incidents are reported to the CPPM immediately. The CPPM determines what additional action must be taken. The ACPPM maintains a record of all incidents. These records are kept as part of the ACPPM security files.

Enclosure (E), U.S. DOE Information Systems Security Incident Form, is provided to facilitate the reporting of incidents.

3. COMPUTER SECURITY RESPONSIBILITY

3.1 Computer Security Organization Within Headquarters

The Computer Protection Plan (Plan) cites the policies, security controls and procedures for implementing the Headquarters unclassified computer security program. This chapter describes the responsibilities of individuals for complying with these requirements. To manage an efficient and cost effective unclassified computer security program, it is necessary to extend the responsibility for protection to all levels of a system(s) life cycle.

The Headquarters Computer Protection Program Manager (CPPM) is the designated representative responsible for developing and managing the Headquarters Computer Protection Program. Assistant Computer Protection Program Managers (ACPPMs) are assigned by organizations to assist the CPPM in implementing the program. Users, application owners, system developers, acquisition and maintenance personnel also play an essential role by assisting in program implementation and compliance.

Whereas previous emphasis was on securing data centers and large custom applications, the most recent issuance of OMB A-130, Appendix III, stresses individual responsibility down to the managers and users of the systems.

3.2 Computer Protection Program Manager (CPPM)

The Headquarters CPPM is responsible for developing and managing a program that includes the appropriate security measures for protection of unclassified mission-essential systems and information. Responsibilities of the CPPM include, but are not limited to:

- Preparing requirements and procedures for the implementation of DOE 1360.2B.

- Maintaining this Headquarters Computer Protection Plan (Plan).

- Performing program oversight to evaluate compliance and effectiveness.

- Communicating security trends, threats, and requirements to organizational ACPPMs.

- Training ACPPMs and assisting them in the implementation of this Plan.

3.3 Assistant Computer Protection Program Manager (ACPPM)

The ACPPM is responsible for coordinating and implementing the Headquarters unclassified computer security program for each unclassified information system (IS) and major application within their organization. Organizations may assign more than one ACPPM based on their area of control, and the number and complexity of systems and applications.

3.3.1 General Duties

ACPPMs perform the following general duties for IS processing unclassified information.

- Ensure the identification of unclassified general support systems, and major and mission-essential applications.

- Perform risk assessments on new systems (before operational), and existing systems and major applications.

- Perform security certification on unclassified computer systems and major applications.

- Ensure implementation of appropriate computer and information protective measures.

- Monitor unclassified systems for the effectiveness of computer security protection measures.

- Review and document comments for new or modified computer system(s) processing unclassified information for adequate protection throughout the life cycle of the system.

- Conduct and participate in computer security reviews.

- Maintain a current inventory of the organization's ISs.

- Participate in the definition of functional security specifications, design reviews, and testing at appropriate life cycle steps in the system development and application development process.

- Ensure the implementation of an appropriate personnel review process for access to unclassified computer systems and major applications.

- Act as the unclassified point-of-contact for contamination incidents within the organization. Notify designated individuals in the event that classified information inadvertently migrates to an unclassified system.

- Establish internal incident reporting procedures and report computer security incidents to the CPPM as outlined in section 2.8.

- Attend ACPPM security training.

- Develop and ensure implementation of a computer security training program for new users, and periodic refresher training for experienced users within their organization.

- Document that new users have received computer security awareness training and are knowledgeable of system prohibitions, protective procedures and security controls.
- Ensure onsite/offsite contractors and subcontractors receive adequate computer security training and comply with the requirements defined in the DOE 1360.2B, this Plan and the NIST Guide, for DOE-sponsored activities under their control.

3.3.2 Processing on Host System

In addition to general duties, ACPPMs in organizations that have networked systems have the following responsibilities.

- Ensure the submission of system Computer Security and Privacy Plans (CSPPs) to the CPPM.

> **Note**: A CSPP is not required for personal computers that are nodes of these networks, and that only access the host to execute applications.

- Maintain the currency of the CSPP and ensure the inclusion within the CSPP of major applications processing unclassified data.

- Implement a risk management process on host system facilities.

3.3.3 Major Applications/Mission-Essential Data

ACPPMs in organizations that have major applications processing mission-essential data also have the following responsibilities.

- Verify the inclusion of the application in the host CSPP.

- Ensure that mission-essential applications are included in the appropriate disaster recovery and contingency plans.

- Ensure organizational participation in tests demonstrating the successful implementation of these disaster recovery and contingency plans.

3.4 System User

Individual users are responsible for implementing the unclassified computer security program and assisting in all aspects of protecting unclassified information from unauthorized disclosure and systems from unauthorized access. Users are also responsible for ensuring the successful recovery of mission-essential information to the extent prescribed in disaster recovery plans.

3.4.1 General Duties

Each user must know the sensitivity of information and mission-essentialness of applications that are in use. The user has the following responsibilities.

- Follow all administrative security measures prescribed for the system.

- Be familiar with the Headquarters and organizational security plans.

- Be knowledgeable of computer security practices and report any occurrence of system abuse or irregularity to the organizational ACPPM.

- Identify information that may require protection.

- Maintain control of all media such as diskettes, cassettes, and printed output containing sensitive information.

- Protect individual passwords.

- Utilize installed system security controls, such as logging off between sessions, to optimize protection of unclassified information.

- Ensure that backups of individual unclassified data files are stored in a secure location to protect them from catastrophic destruction.

- Ensure backups are identified and labeled as to the date of backup, sensitivity of information, the system it was created on, and the type application that generated the data.

- Use care in labeling sensitive media with the type of data that is contained therein, i.e., for Official Use Only, Privacy Data, etc. The need-to-know should be a greater concern for sensitive data contained on large volume media, such as Zip drive cartridges, where the volume of data loss is a higher risk. (See section 5.4.1.1)

- Ensure proper clearing of information storage media to restrict unauthorized and inadvertent access and disclosure.

- Ensure that systems determined to be mission-essential are identified to the ACPPM.

- Ensure that major applications are identified to the computer system manager and are included in organizational contingency planning.

- Utilize DOE equipment for official government activities only. Do not use equipment in an abusive, disruptive or fraudulent manner.

- Submit suggestions for improving computer security to the ACPPM.

3.4.2 Standalone System User

The accountable user is responsible for protecting standalone computers within the controls prescribed in this document. Test equipment that accesses and captures sensitive data from an unclassified system requires the same protection as a personal computer processing sensitive information.

3.4.3 Network User

Individual users are responsible for access security through their individual node and protection of their password. Personnel accessing unclassified information through a network must be cognizant of, and compliant with, the security controls and procedures prescribed within the networked system security plan.

3.5 Organization Program Manager

The organizational Program Manager, typically a Division Director or Group Leader, has the overall responsibility for oversight for IS programs under their purview, whether they are directly involved or the responsibility has been delegated to others. The Program Manager has the general responsibility for the organization supported by the computer system and/or application. Their responsibilities include the following.

- Ensure the designated official, who administers an information system for the Program Manager, is responsible and accountable for the management of that system throughout its life cycle.

- Authorize, in writing, the use of each computer system based on implementation of its security plan before beginning or significantly changing processing in the system. Use of the system will be reauthorized every three years.

- Authorize, in writing, the use of each application by confirming that the security plan, as implemented, adequately secures the application. Results of the most recent assessment or review of controls will be a factor in management authorizations. The application must be authorized prior to operating. Management authorization implies accepting the risk of each computer system used by the application.

- Authorize major applications every three years, but more often where the risk and magnitude of harm or loss is high. The intent of this requirement is to assure that the Program Manager, whose mission will be adversely affected by security weaknesses in the application, periodically assesses and accepts the risk of operating the application. The authorization should be based on the application security plan and any review(s) performed on the application. It should also take into account the risks from the computer system used by the application.
- Approve applications/systems to operate based on the CSPP and the security certification, when necessary.

Authorization granted by a Program Manager for a system to process information (accreditation), is an important quality control. By authorizing processing in a system, a manager accepts the risks associated. Authorization is not a decision that should be made by the security staff.

3.6 Organization Computer System/Application Owner

The owner of a computer system or major application is responsible for determining the sensitivity of the data being processed. In addition, the data owner must establish the need-to-know criteria and access restrictions. Responsibilities include the following.

- Identify unclassified information that may be sensitive and require protection.

- Identify applications determined to be mission-essential.

- Incorporate mission-essential applications into the organizational contingency planning process.

- Incorporate computer security requirements into system and application development and support requirements.

- Participate in the personnel screening process by verifying (either personally or through a procedure) the need-to-know of each requester for application access.

- Establish a process for initial enrollment of users into the application, periodic assessment and verification of continued need, and immediate notification and deletion of users who no longer require access.

3.7 Computer System or Application Developer/Maintainer

The system or application developer and maintainer is responsible for developing and maintaining a system or application in accordance with established policy and security guidelines to ensure that the system/application supports required security measures. The developer/maintainer has the following responsibilities.

- Incorporate appropriate protective measures that address security requirements into the system/application.

- Include testing of security features in the system/application test plans.

- Delete test data, passwords, and development and testing access prior to system/application migration to operational use.

- Develop documentation that supports application security certification and system approval.

3.8 System and Major Application Acquisitions

Personnel involved in the acquisition of computer systems, and major and mission-essential applications that process unclassified information will ensure that the requirements for personnel assurance screening, specialized protection requirements, and security measures are considered in each procurement action.

4. INFORMATION SYSTEMS REQUIRING PROTECTION

4.1 Computer System/Application Identification

Organizations must identify computer systems and applications that require protection through their Assistant Computer Protection Program Managers (ACPPMs). ACPPMs ensure that computer systems and major applications are included in contingency and disaster recovery planning, and have a Computer Security and Privacy Plan (CSPP). The CSPP becomes an attachment to this Plan when completed. Significant changes to individual systems and applications are indicated in revised CSPPs and resubmitted to the CPPM.

Enclosure (C), Computer Security and Privacy Plan Outline, contains an outline which defines the individual system elements to be completed for the CSPP.

4.2 Types of Information and Systems Requiring Protection

All computer systems are considered to process some sensitive information (OMB A-130, Appendix III), and therefore require a CSPP. Major applications are typically mission-essential, and therefore require both a protection plan and a continuity of operations plan. Sensitive information is information that must be protected to ensure its confidentiality, integrity, and/or uninterrupted availability. The extent of protection should be commensurate with the risk and magnitude of the harm that could result from the loss, misuse, or unauthorized access to or modification of information.

4.2.1 Information Systems Sensitivity

Sensitive unclassified information requires protection from unauthorized disclosure, unauthorized or unintentional modification, and must be available on a timely basis to meet mission requirements or avoid substantial losses. Types of sensitive data include rights of interest; legal; proprietary; sensitive energy, financial and budget data; and other types of data that require protection under law, contract, or Federal policy.

4.2.2 Mission-Essential Information

Mission-essential applications are critical to the mission of the Department and/or organization. A computer-based application or system is essential if its interruption or denial of access would have an adverse impact on functions necessary for the continuous operations of DOE and the Federal Government. These systems and applications, and the names of their owners, are included in individual organizational contingency plans and/or CSPPs.

4.2.3 Major Application

An application is major if it requires special management attention because of its importance to the Department's mission; its high development, operating or maintenance costs; or its significant role in the administration of Departmental programs, finances, property or other resources. Major is synonymous with mission-essential.

4.2.4 Unclassified Controlled Nuclear Information

Unclassified Controlled Nuclear Information (UCNI) has control and protection requirements mandated by DOE Order 471.1, *Unclassified Controlled Nuclear Information*. Any Headquarters system processing UCNI must incorporate the security features of this Plan in addition to the controls mandated by the UCNI order.

4.2.5 Scientific and Technological Information

The data owner and ACPPM determine the controls for scientific and technological information. Any system processing this information must have additional security measures and controls as directed by the owner, in addition to the minimum requirements outlined in this document. The DOE Office of Scientific and Technological Information (OSTI) issues any additional requirements and instructions for this type of information.

4.2.6 Official Use Only Information

Information that is identified as "Official Use Only" by any Federal Government or DOE entity will be offered the same level of protection as assigned by the issuing activity. At a minimum, this information will not be made available for public dissemination without the permission of the information owner or issuing agency.

5. SECURITY CONTROLS

5.1 Overview

Organizations are required to prepare Computer Security and Privacy Plans (CSPPs) for each system, or group of similar systems (except personal computers (PCs)), processing unclassified information and mission-essential applications. Organizations designate Assistant Computer Protection Program Managers (ACPPMs) to assist the Computer Protection Program Manager (CPPM) in maintaining security controls in the Headquarters program.

Protective measures are typically categorized as administrative, technical, physical, and personnel. Controls within each category collectively provide reasonable and cost-effective protection of computer assets. Some controls are universal and others are system-specific. For example, the contract guard force and physical access controls are already in place for the Germantown and Forrestal facilities. They offer a degree of physical protection for all computer systems within the DOE Headquarters IS facilities. Conversely, the Access Control Facility 2 (ACF2) information security system provides password protection specifically to files residing on mainframe computer systems. It offers no protection to local area networks (LANs) in the same physical facility.

Diverse system configurations require different methods of protection, depending on the points of greatest risk. Protection measures should be commensurate with risk to exposure. For example, a system located in a controlled exclusion area requires less local physical protection than one located outside an exclusion area. Another example would be implementation of file encryption on a shared PC hard drive device to protect individual user files from other authorized users.

5.2 System

For the purpose of this Plan, the term "system" is defined as a collection of people, machines, and methods organized to accomplish a set of specific functions used in the automatic acquisition, dissemination, collection, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information. A system includes the following:

- computers
- hardware
- software, firmware, and similar procedures
- services, including support services

5.3 Computer System Environment

For the purpose of grouping similar system security features, computer system security controls are based on their operating environments. In this Plan there are two operating environments: standalone and networked. The major difference is that in a standalone environment the security threat is localized, whereas in a network the threat is global. All systems, to a degree, have nodes, paths, and applications.

5.3.1 Standalone System Environment

The standalone system environment includes a self-contained processor and local peripherals (printers, drives, etc.), where processing and security is unilaterally controlled by the user in the standalone mode. For physical controls, microprocessors are considered standalone, and networked when operating in a network environment. This may be further divided into the two categories shown below.

- **Fixed Operation**. An environment wherein all processing and data access are logically restricted to a processor and location in a standalone mode. Set up is a stationary environment, such as an office or data center, where users have control of all resources. An example of this is the personal computer.

- **Portable System**. This equipment is self contained and independent of any other support. It is mobile and may be run on battery power. This includes some computerized test equipment, and laptop and notebook computer hardware. While portability and size may make protection easier, the threat of physical loss and unauthorized access increases due to the nature of design and purpose.

5.3.2 Networked System Environment

A networked system environment may contain many functionally connected workstations, processors and peripherals distributed over an expanded area (room, building, campus, etc.). A system administrator is responsible for controlling access to information through the allocation of system privileges. On a local area or wide area network, the typical user accesses the file server, downloads programs and/or files, and processes remotely. There is a capability to communicate with other users, share files, and transfer information. A specifically configured processor is dedicated as a network server. Mainframe systems, consisting of one or more mainframe computers or minicomputers, with peripherals and supporting equipment, and contained in a central room or facility, may be connected to the network.

This type of environment receives the most attention for protective features by virtue of historical reliance on mainframe computer operations. In addition to system controls, access can be restricted at remote workstations with physical controls and office restrictions. On the mainframe, individual or specific access to data is controlled more by sets of system rules than by local administration. A system administrator normally defines and assigns terminal access and system privileges.

5.4 Minimum Security Requirements

Unclassified computer system security controls will be determined by the risk and threat to the environment in which the information is accessed, processed, or stored. Based on a general risk and threat scenario, this Plan specifies the minimum security controls that must be employed when processing unclassified information on Headquarters systems. Other comparable measures may be substituted if the risk is reduced proportionately. Use of substitute measures are proposed to, and approved by the system owner's Program Manager. Additional controls must be used if the risk warrants.

5.4.1 General Security Measures

DOE Federal and contractor employees will use only officially approved software on systems provided for their use, and must comply with agreements for that software license. Program Managers will ensure that employees are using Federal information processing resources for officially approved activities, and that they are made aware of software requirements and the potential harm which could occur from willful infringement of those licenses. Systems processing unclassified information require the following security measures.

5.4.1.1 Administrative Security Procedures

- **Need-to-Know.** All personnel within the immediate work area having visual access to the data, and personnel accessing the data, must have a need-to-know for the information being processed.

- **Awareness.** All users will be aware of the contents of DOE/HR-0145, *Your Responsibilities as DOE Employees* (Under the Privacy Act (PA) and Freedom of information Act (FOIA).

- **Marking Media and Documents**. When practical, removable storage media should be marked externally for physical protection at the processing location, and internally if the data is transferred across a network. This is especially a concern for large capacity media, such as Zip drive cartridges, where the risk of data loss is much higher. If sensitive and non-sensitive data are stored on the same removable magnetic media, the media should be marked at the highest level of sensitivity of the information contained therein. However, it would be more prudent if media containing sensitive data were to be segregated from media containing non-sensitive data. Segregate different types of data (e.g., unclassified weapons data and waste management data should not be contained on the same diskette or cartridge that contains general administrative type data.)

  Printed data determined to have a degree of confidentiality will either be marked on the first page, or have a cover sheet attached identifying the data sensitivity and handling instructions prescribed by the information owner.

- **Printers.** Precautions must be taken to ensure that the printer does not store sensitive data in memory or buffer space and produce residual information after a printing job finishes. If possible, the printer buffer should be cleared of any sensitive data that may still be in memory. When printing sensitive information on a shared printer, the printer must be attended. If unattended, the room where printing is performed must be controlled.

- **Maintenance.** Maintenance personnel must have a need-to-know for the category of information residing on the system, or be supervised by an authorized individual when working on a system.

- **Access Control.** Access to the system must be protected. This can be done by using a password feature or locking device that denies use of equipment and access to unclassified information by unauthorized users.

- **Password Protection.** Sharing a password, when used as a protection feature, ***is prohibited.*** Keywords, such as those used for file access on media, are not passwords in the context of this document.

- **Document/Media Control.** All documents and media containing unclassified sensitive information must be controlled and protected from unauthorized viewing. These items will not be exposed or provided to individuals not having a need-to-know.

- **Screen Display.** The display screen will be protected from view by the casual passerby during processing of sensitive information. The system may not be left unattended when in use and the user must log off when leaving the system.

- **Terminal Time Out.** Terminals will incorporate an automatic time out feature that deactivates or masks the screen to preclude viewing in the event the user leaves the terminal unattended.

5.4.1.2 Training

Compute security training is required for all individuals accessing DOE ISs or computers containing DOE information. (See Chapter 9)

5.4.1.3 Contingency Planning and Back-Up Operations

All computer systems that are processing major applications, as identified by the computer system manager, must be included in a disaster recovery plan. Mission-essential applications must have a contingency plan in place. This may be as simple as backing up data at the individual workstation and storing out of the area. It can be as complex as having mainframe system backup, offsite storage, full "hot site" recovery, and continuity of operations plans. Every user is expected to be familiar with the contingency plan for operations of their specific system and application, and the procedures for information retrieval in the event of contingency plan activation. (See Chapter 8).

5.4.1.4 Magnetic Media Clearing

All magnetic media retired from use, removed for trade, sale, excess or destruction, or sent out for maintenance must be cleared of all data (regardless of whether it is sensitive or not), and all application software. This may be done by low level formatting the media, overwriting the information or degaussing.

5.4.1.5 Destruction of Media

Hardcopy and magnetic media containing unclassified information will be modified, erased, or destroyed in a manner consistent with the Headquarters Facilities Master Security Plan, Chapter XI, Section 13.a, Destruction, to prevent the reuse or recovery of information from the media.

5.4.1.6 Incident Reporting

Elements of a significant incident nature are defined and reported in accordance with the procedures outlined in Attachment 3 to DOE 1360.2B.

> Attachment 3 to DOE 1360.2B is included in this Plan as Enclosure (E), Information Systems Security Incident Report, to facilitate the reporting of incidents.

5.4.1.7 Risk Assessment

Revised OMB A-130 makes the assumption that all unclassified systems contain some sensitive information. It also changes OMB's requirements for a formal risk assessment to one of an internal, self assessment nature. The responsibility for adequate security for organization’s information systems will reside with the Program Manager responsible for the computer system and/or application within their program area.

The informal self assessment process gives the Program Manager flexibility for assessing and documenting risk on new systems before operational use, and existing computer installations processing unclassified and mission-essential information. Risk should also be assessed on existing facilities every 3 years, or whenever there is a significant change to the existing system.

> See DOE 1360.2B, section 11.c (Management Control Process), and section 11.f (Risk Assessment Process), for further guidance.

5.4.2 Controls for Standalone Computers and Their Peripherals

5.4.2.1 General Controls

General controls to be applied to all processors processing unclassified information are described below.

- Headquarters automated information may only be processed within the physical bounds of DOE Headquarters, other Federal Government locations, or DOE Headquarters approved contractor facilities. Processing of information outside of these facilities is prohibited unless specifically authorized by the Program Manager responsible for the application being accessed.

Authorization for offsite processing may be granted by using the form in Enclosure (F), Authorization for Official Business Use of Computer Resources.

(a) Departmental computer processors, terminals, microcomputers/word processors, software, and data will only be used for official business. A written authorization signed by a Program Manager is required before offsite work is considered official business. Authorization will be given contingent upon written agreement on adherence to DOE policies for security, management of software, data, records, property, and employees' work place, hours of work, and appropriate compensation (to include software and hardware maintenance).

(b) Use of privately-owned terminals, microcomputers/word processors, and software on or offsite will be considered DOE official business when preauthorization is given in writing by a Program Manager, and a written agreement is signed by the employee on adherence to DOE policies for security, management of software, data, records, property, and employees' work place, hours of work, and appropriate compensation (to include software and hardware maintenance).

(c) All data authorized to be prepared for Departmental work using processors, terminals, and microcomputers/word processors, regardless of the ownership or location of the equipment, are the property of the Department of Energy and are considered official records. This includes job-related work authorized to be done at home on privately-owned computers. All official records must be retained as required and backed up. Adherence to software license agreements must be observed.

(d) Preauthorization will include informing the employee about potential liability contained in Public Law 99-474, the Computer Fraud and Abuse Act of 1986, and the requirements of 10 CFR 1010.207, Use of Government Property.

(e) A portable computer system is prohibited from processing information unless appropriate accountability and control procedures are established to deter the compromise of the system and the media. All portable systems will have a virus detection program installed prior to processing information. The Human Resources and Administration's Office of Information Management (HROIM) provides installation and instructions on the use of virus detection software programs such as the Norman Data System products and DOEVSTOP. Headquarters Elements will stress the importance of proper precautions to safeguard portable computers while in a travel status (i.e., never leave the items unattended, hand-carry on airplane, record serial number and/or DOE tag number, etc.)

- Access to each processor is to be limited. Know all persons who use, service and repair the processor. Demand identification and authorization from anyone who wants to remove a PC or hard disk for maintenance.

- Passwords, when used, will not be shared and will be protected.

  (a) Keys and passwords to equipment processing information will be protected from unauthorized use.

  (b) Passwords will be composed of random characters; do not use names, nicknames, social security numbers, phone numbers, names of family members, or words that are easily guessed (i.e., protect, security, password, etc.).

  (c) Passwords are to be changed at least every 6 months.

  (d) Passwords should be memorized; however, if an operational need arises to write the password down, then it must be stored in a locked file cabinet or security container.

  (e) Using script or macro files that contain USERID and password combinations to access host systems is prohibited.

- Unauthorized software packages (demonstrations, games, etc.) and non-government related personal information are prohibited on DOE computers.

- Unauthorized copying of commercial software using DOE resources is prohibited. Software license agreements for every software package are to be strictly obeyed.

- When processing information while connected to another computer system, all systems will comply with the controls defined in the CSPP of the host computer system or network.

5.4.2.2 Unclassified Processing Controls

In addition to the general controls, the following controls will be employed when processing unclassified sensitive data.

- Each system, including peripherals, must meet at least one of the following criteria.

  (a) Be composed of exclusively removable media (i.e., no fixed hard drive) that is removed and stored when not in use.

  (b) Be capable of having the system or disk drive locked to preclude unauthorized access.

  (c) Have installed a software or hardware security package that offers reasonable protection to files (this may be a password control, data encryption or a file protect package).

(d) Be contained in a controlled area where only personnel with a need-to-know may enter unescorted.

- A portable system is prohibited from processing or retaining sensitive data offsite, except under the following conditions.

  (a) Authorization must be granted by a Program Manager. This authorization must be on file with the ACPPM and contain the specific circumstances as to where and how this information is to be controlled.

  (b) The system will be either hand-carried or shipped as controlled baggage when traveling on a commercial carrier.

  (c) The data or media will be secured at the nearest government facility or stored in an area that offers reasonable protection (e.g., when it is necessary to take information media into a commercial hotel, it will be secured as valuables when not in the possession of the authorized holder).

  (d) Sensitive data will be removed from the system and fixed media will be cleared prior to reuse by another user unless that user has a valid need-to-know for the contents.

  (e) Appropriate accountability and control procedures will be established to deter the compromise of the system and the media.

- Sensitive information will be limited to individuals with an established need-to-know and during the conduct of official business. The IS will be protected or cleared of sensitive material prior to reuse.

- PCs and their peripherals will not be left unattended when processing sensitive unclassified data unless appropriate controls have been implemented.

- Computer screens will be protected from casual, unauthorized viewing during sensitive information processing.

- Policy dealing with the removal of single-strike or multi-strike printer ribbons is a local decision by the ACPPM.

- All storage media and output should be properly identified and marked conspicuously when sensitive information is resident (e.g., Official Use Only, Privacy Data, Proprietary Information, etc.). (See section 5.4.1.1)

- All storage media and printouts containing sensitive information must be appropriately stored to prevent unauthorized viewing (e.g., in a locked file cabinet, security container, or locked desk drawer), when not in use.

- Destruction of sensitive materials should follow methods used for classified destruction. The use of the regular trash or recycle containers for disposal of sensitive information is prohibited.

5.4.2.3 System Backup

Backup copies of mission-essential data files will be made frequently. The copies will be stored in such a manner so each media is recoverable in the event of a disaster or contingency.

5.4.2.4 Networked IS

Any host IS may list additional security controls for PCs and their peripherals in their respective CSPPs when they are used as terminals to the networked IS.

5.4.3 Network System Security Controls

Networked systems must have physical, administrative, and environmental protection measures in place commensurate to the data processed and the threat to the physical plant. Additional technical security controls are implemented within the system to limit access, identify media, and support audit trails. For the purpose of this document, a networked system includes minicomputer, mainframe, dial-in, wide area network (WAN), local area network (LAN), metropolitan area network (MAN), and/or collegiate network systems. In addition to the General Security Measures (5.4.1), and the Controls for Standalone Computers and Their Peripherals (5.4.2) of this Plan, the network environment includes the following minimal security features.

5.4.3.1 Responsibility

The system user has the primary security responsibility for ensuring that all security features are functioning properly at their workstation. The user must abide by the rules set down by the Network's CSPP. The network system administrator is assigned in writing and is responsible for security of the network. Overall system security responsibility must be predetermined and coordinated when accessing different networks.

5.4.3.2 Protective Measures

A networked system incorporates the following features.

- **Audit Capability**. The system possesses an audit trail capability to identify and record system sign-on and file/database access. The system supports and records the auditing features that documents who is accessing the system (identification), from where the system is being accessed (port/source), the time of access, and the files accessed. Unsuccessful logon attempts will be detected and recorded.

- **System Access and Termination**. The data owner determines the need-to-know. The ACPPM ensures the existence of a procedure to authorize all host access for legitimate users and terminate access for personnel who no longer have a need.

- **Password Protect**. The system will be password protected. A password will consist of a minimum of 6 alphanumeric characters and not be a dictionary or easily guessed word. It must be changed a minimum of every 6 months or when an individual transfers or employment terminates. Privileged passwords are restricted to the system administrator with a protected copy available to the system manager in case of an emergency. A supervisor password must be changed a minimum of every 3 months.

- **Identification and Password.** Users will be assigned a unique identifier and a protected password. Users with supervisor privileges will have one password for supervisor access and one for routine use. The issuance of supervisor privileges will be kept to a minimum.

- **Forced Password Change.** The system should force an individual password change at least every 6 months. Privileged passwords are changed at least every 3 months.

- **File Access.** Individual data files identified as containing sensitive information will be protected from indiscriminate access by users on the network.

- **System Warning Notice.** Every system will display the following notice on the first screen prior to entering the system:

  WARNING

  To protect the system from unauthorized use and to insure that the system is functioning properly, activities on this system are monitored and recorded and subject to audit. Use of this system is expressed consent to such monitoring and recording. Any unauthorized access or use of this Information System is prohibited and could be subject to criminal and civil penalties.

- **Output Media Marking.** Sensitive hardcopy output files and information will be visibly marked as to the sensitivity and handling instructions of the information produced. This may be done with a cover sheet or on each page. Removable magnetic media is prominently labeled as sensitive. New or major application modifications should include marking the sensitivity of the media via software, to the maximum extent possible.

- **Internal Marking**. To the maximum extent possible, the data and individual display screens will identify sensitive information.

- **Memorandum of Understanding.** In the event the network will cross domains through a link into another network, a memorandum of understanding (MOU) will be made between the responsible security administrators. This MOU is required when an external agency or organization will access Headquarters systems.

- **Security Level.** Any networked system must follow the rules for the highest sensitivity and most restrictive nature of information, as identified by the information owner, that is accessible by the individual workstation.

- **System Backup**. The system will have scheduled backup that will be retained in secure storage, such as a vault or offsite location, in case of a catastrophe.

- **Public Path Password Protection.** Passwords transmitted over public access paths should be encrypted, utilizing a DOE approved methodology.

5.5 Non-DOE Personal Computer Security

Government-controlled information will not be processed or stored on a personally-owned or non-government-owned personal computer without the approval of a Program Manager. The information remains the property of the U.S. Government.

5.6 Software Application Development/Modification

Software application development or modification will be in accordance with the DOE Guide 200.1-1, *Software Engineering Methodology (SEM)* or another equivalent guide.

6. COMPUTER SECURITY AND PRIVACY PLAN

The purpose of the Computer Security and Privacy Plan (CSPP) is to identify the level of protection required for unclassified computer systems and applications and to document the specific computer security environment not covered in the NIST Guide. Information from the CSPPs is reviewed during assistance visits by the CPPM to determine if protection measures are sufficient for each system or application. The CSPPs also serve as a management tool for determining allocation of available assets, assistance and effort.

When using the individual CSPP format and the information requested does not apply to your system or application, enter "Not Applicable" or "N/A" in the space provided. When completed, some system CSPPs will list major applications and identify the host system on which it resides.

All plans are reviewed by the ACPPM on an annual basis, and the CPPM reviews the plans every three years. Any significant changes to the system or application, such as redesign or enhancements, may affect security features and must be indicated in a revised CSPP, be certified by the ACPPM and approved by the Program Manager.

An outline and contents for the CSPP can be found in Appendix "A", NIST's *User Guide for Developing and Evaluating Security Plans for Unclassified Federal Automated Information Systems*. The NIST document was developed to guide Federal agencies in developing security plans for Federal ISs, and should be used in place of the previous Plan's Chapter 6.

Enclosure (C), Computer Security and Privacy Plan (CSPP) form, contains the instructions previously found in this section.

7. RISK MANAGEMENT PROCESS

7.1 Requirements

OMB Circular A-130, Appendix III, no longer requires the preparation of a formal risk analysis. It does, however, require an assessment of risk as part of a risk-based approach to determining adequate, cost-effective security for a system. The risk management process is required for all new or significantly modified Headquarters unclassified computer installations, whether centralized or networked. It will be structured for the specific installation being assessed. The risk assessment process may vary in scope based on the sensitivity of the information being processed, and the complexity and size of the system.

The risk assessment process provides an evaluation of the system assets and related risks, hazards and threats, so that security resources may be effectively distributed to minimize potential loss. Existing security safeguards are evaluated based on the effectiveness of protecting the information, and additional safeguards are assessed so a cost-effective selection may be made to reduce exposure. The CPPM may also require that the risk management process be conducted if a major compromise or incident occurs that demonstrates a weakness in the security of the facility.

7.2 Responsibility

Risk assessment and risk management are crucial elements of the security planning process. The Headquarters IS risk management program consists of the DOE Site Statement of Threat and the facility risk management process. The risk management process for DOE Headquarters installations processing unclassified information follows the NIST Guide, Section III.A, Risk Assessment and Management. It includes the risk assessment content.

The organization's ACPPM will review previous risk assessment documents relative to their organization. The actual effort should be performed by the system/facility manager, ACPPM, and technical staff. The CPPM provides assistance in the conduct of the risk management process, as requested. Risk assessment documentation is reviewed by the ACPPM as part of the IS certification process.

8. CONTINUITY OF OPERATIONS PLANNING

8.1 Management Control and Responsibility

A goal of the DOE Headquarters Computer Protection Program is to ensure that a continuity of operations decision is made for all systems, applications and information. Those determined to be mission-essential should be included in a **Continuity of Operations Plan (COOP**). The COOP includes plans for recovery in the event of total disaster and planning for contingency operations. The COOP, and individual organizational plans, outline recovery authorities and responsibilities. Planning considerations include the actions to be taken prior to realization of a contingency situation, action during the event, and recovery operations. Facility managers, system owners and users are all an integral part of the Headquarters COOP program. The CPPM reviews the existing organizational guidance to evaluate the completeness and effectiveness of their planning. Plan readiness and compliance are evaluated during the normal update and review of organizational Computer Security and Privacy Plans (CSPPs).

8.1.1 Facility Manager

The manager of an IS facility, such as the Germantown Administrative Computing Center or the Germantown-based Headquarters Local Area Network Backbone, has the responsibility to develop a disaster recovery plan for their facility and physical plant equipment. The manager is also responsible for including in the facility plan, plans for the mission-essential applications they are supporting, or to inform the system owner if they do not have a plan. The disaster recovery plan defines the computer center recovery team's structure and organization, and identifies responsibilities of specific teams and individuals. Detailed procedures will be listed and followed by each team under various contingency scenarios, and computer operations personnel to restart essential applications.

The facility manager publishes the disaster recovery plan. The plan will contain the individual application contingency plans. Major system/application owners will be kept informed of any changes to the host system disaster recovery plan that may affect their operations. The facility manager plans for all computer systems under their responsibility, unless specifically exempted by the system owner or Program Manager. Software applications running on equipment in the central computer facility are included in the facility contingency plan. The system/application owner retains the responsibility to ensure that an updated version of an application is readily available in the event of a contingency.

8.1.2 System Owner Contingency

Contingency planning is performed by individual user organizations for their applications. The owners of mission-essential systems and applications are responsible for developing total disaster recovery planning and contingency planning for the system and information being processed. When mission-essential information resides on a host system, the system owner must ensure that the host system Continuity of Operations Plan (COOP) includes contingency planning for their data, or have an alternative plan. They must develop a contingency plan that supports continued user activity during the interim period of host restoration of operations. In addition, computer system owners must ensure that application owners are aware of the limitations of processing support during periods of outage and degraded operating modes, and include these considerations in their individual contingency planning.

8.1.3 System User

The individual PC user has the responsibility for ensuring that any mission-essential information on their system is backed up and stored in a safe location. Additionally, they are responsible for having a plan to return their system to an operational mode in case of catastrophic failure. This can be coordinated through the system owner or the ACPPM.

8.2 Headquarters Unclassified Systems

This Plan requires contingency planning for Headquarters major applications and general support computer systems, and disaster recovery planning for processing facilities. Facility managers and system and application owners are responsible for ensuring that contingency requirements are addressed during the requirements definitions phase of development for all Headquarters systems and applications determined to be mission-essential. Planning responsibility is passed on to the ACPPMs for their respective systems and applications.

8.2.1 Sensitive Information

Because OMB Circular A-130 considers that all systems contain some sensitive information, all unclassified information will be protected during continuity and recovery operations with the features outlined in this Plan.

8.2.2 Mission-Essential Applications

Applications determined to be mission-essential will have data backed up and stored in a protected location, as determined by the owner. This is in the event the primary processing location becomes unusable due to disaster, maintenance, or civil disobedience.

8.3 Contingency Planning and Implementation

The CPPM has the responsibility for ensuring that procedures are in place to protect Headquarters systems and information from unauthorized access and inadvertent loss. To this extent, the CPPM provides requirements and performs Headquarters oversight.

The ultimate responsibility for contingency planning and subsequent action lies directly with the organizational system/application owner. ACPPMs are designated to accomplish this task. The following outline of planning considerations and actions is provided for guidance to help the ACPPM accomplish this task.

8.3.1 Considerations

The most important process of contingency planning is defining potential problems and making decisions before an event occurs. Every contingency is unique, but there are certain fundamental decisions that will aid in the continued operation, processing, and recovery of data. The following questions will assist in planning for an expeditious recovery.

8.3.1.1 Assets Requiring Protection

Identify your most valuable assets that may be affected by the different types of disasters or outages. These might be one or more of the following.

- Hardware
- Software
- Information
- Work continuity

8.3.1.2 Survivability Time Frames

How much time can pass before the loss of the asset has a detrimental effect on your operation and to what degree?

- Short-term (as defined the data owner)
- Long-term (as defined by the data owner)

8.3.1.3 Contingency Implementation Considerations

There are many reasons for implementing a contingency plan.

- **Contingency Event.** A viable plan should consider, at a minimum, action to be taken in any of the following instances.

  a. Power Outage
  b. Bomb Threat
  c. Weather
  d. Loss of Technical Support
  e. Loss of Communications
  f. Loss of System
  g. Fire
  h. Hostage/Barricade situation
  i. Water hazards
  j. Software Error

- **Who are the responsible individuals?** Identify the individuals who would most likely be contacted in the event a contingency plan is implemented. An office telephone number is preferred to a specific individual. At a minimum the following persons will be identified.

a. Owner
b. User
c. Support contractor developer/maintainer
d. Technical Support (include system administrator)
e. Emergency maintenance (building engineers for power, etc.)
f. Security

- **Who can help you?** Conduct initial research to identify other persons or sources to assist you in the execution of a contingency plan. The below listed offices may expedite the recovery process and ultimately reduce the administrative effort.

a. Procurement
b. Budget
c. Other organizations with similar and compatible systems

- **What is available?** Predetermine comparable assets that may be readily available to replace inoperative or inaccessible equipments or services. This can include agreements between similar system users to provide service in the event of a contingency implementation. These assets may include the following items.

a. Hardware (backup equipment, server, drive, etc.)
b. Communications (alternate paths)
c. Software (operating system, applications, backup data files)
d. Comparable equipment/systems (availability and for how long)
e. Support personnel

- **Extent of contingency.** Divide the planning into executable increments dependent on the extent of contingency realization. Specific portions of the plan may be required for partial or short-term outages whereas full plan implementation is required for total long-term denial of service. Considerations would be for full contingency (worst case scenario), or partial contingency (what portion of the plan will be implemented).

8.3.2 Actions to be Taken

There are normally three phases to consider in preparing a service disruption planning document: before; during; and after realization of the event. Some areas of planning may overlap whereas others may be specific to that particular period of time.

- **Phase 1: Before the Occurrence of a Disaster.** This is the planning phase. When planning for the restoration of service, emphasis must be placed on developing detailed procedures, coordinating actions and exercising the process. At a minimum, this should include the following.

a. Preliminary planning
b. Preparation
c. Assignment of responsibilities
d. Develop and finalize the plan
e. Plan approval (management acceptance)
f. Full or partial plan testing
g. Distribute copies of the plan containing duties/actions

- **Phase 2: During the Event.** Once the event occurs, instructions will be readily available to all activities and people included in the plan. The goal at this time will be the recovery and continued operations of essential services. The following would be considerations and activity at this time.

  a. Availability of instructions
  b. Implementation of individual contingency plan(s)
  c. Continuity of operations

- **Phase 3: After the Event.** Once the event occurs and temporary service resumes, the following considerations and action should be addressed.

  a. Relocation (if required)
  b. Restoration of normal operations (resumption)
  c. Lessons learned (modify plan)

8.4 Review and Maintenance of Disaster Recovery/Contingency Plans

Contingency planning will be reviewed annually by the ACPPM. Contingency plans will be reviewed to ensure all upgrades to the system environment and the names and telephone numbers of responsible individuals are current.

- Annually
- Periodically (what is a practical review period)
- Continually (as events occur etc.)

Completeness of disaster recovery plans can be evaluated by filling out the Emergency Readiness Evaluation Questionnaire in Enclosure (D).

8.5 Testing

The plans for essential systems are tested at least every three years. Portions of the plan should be tested annually or when significantly modified. The essentialness and complexity of the system determine the degree of testing to be accomplished.

- Partial & Full (if practical)
- Plan effectiveness
- Make improvements

8.6 Contact Lists and Emergency Notification Procedures

Individual disaster recovery and contingency plans contain the key points of contact to be notified in an emergency to include security, operations, and maintenance staff. System emergencies involving security are reported to the individual exercising security responsibility for that system or facility. All other emergencies are handled by computer operations personnel.

Emergencies requiring police, fire and rescue and building maintenance for DOE controlled spaces are initially reported and handled through the building guard force. Emergencies in contractor-controlled spaces are handled as described in the contractor's contingency or disaster recovery plan.

9. TRAINING

9.1 Management Concept

The Headquarters Computer Protection Program Managers' (CPPM) approach to computer security awareness and training is to distribute training materials, train the Assistant Computer Protection Program Manager (ACPPMs), evaluate program effectiveness, and delegate to each ACPPM the authority to develop their own training programs. The CPPM establishes the minimum training to be accomplished, and may provide materials.

9.2 Computer Security Training

Computer security training begins with the initial security indoctrination given by DOE Headquarters security, which is required of new employees and onsite contractors. Security training continues at the organizational level with, at a minimum, a briefing to the user by the ACPPM prior to accessing a DOE Headquarters computer workstation. Security awareness is a continuing process with security notices and updates disseminated through periodic publications, bulletins, and refresher briefings.

9.2.1 Headquarters Indoctrination

DOE security provides security training for all newly hired employees. This training encompasses information security, marking and handling of documents, visitor access controls, and escort procedures.

Individuals will receive additional security training at the organizational level when assigned a computer workstation. At a minimum, this will consist of a briefing by the ACPPM or designated security administrator. The individual is given training materials for awareness and reference.

Individuals assigned duties as computer security escorts will receive briefings on their responsibilities and the expectation of the assignment. At a minimum, this will consist of the degree of sensitivity involved, the vulnerability of information exposure by unsupervised but authorized program access, and the physical location of access points.

9.2.2 Department of Energy Training

Headquarters developed the Guideline for Development of Unclassified Computer Security Awareness and Training Programs, DOE/MA--0320 dated February 1988, for use by all organizations in training their personnel in computer security.

The NIST Guide, Appendix "A", contains more detailed guidance.

9.3 Security Awareness

Throughout the Department there are posters displayed promoting security awareness. When computer security warnings and alerts are appropriate, they are posted electronically on OfficeVision, Time-Sharing Options (TSO), and LANs (CC-mail). Security bulletins are issued by the Department on relevant security issues as necessary.

9.4 Continued Training

A required security refresher briefing is given annually for all employees and contractors by DOE Headquarters. The individual computer system owner provides supplemental security information concerning the proper use of specific security controls.

Computer center personnel receive additional training in emergency response and restoration and recovery procedures, as detailed in the DOE Headquarters Administrative Computer Center Continuity of Operations Plan.

9.4.1 Headquarters Computer Security Training Courses

Headquarters provides computer security training on system rules and controls to mainframe application owners and users, such as those implemented on ACF2.

9.4.2 Viruses

The HROIM conducts periodic virus seminars on the presence, detection, and prevention of viruses that have been detected within DOE Headquarters facilities.

Additional information on viruses can be found on the Headquarters Automated System Security Incident Strike Team's website, *http://www-it.hr.doe.gov/ASSIST*.

9.5 Training Materials

There is an abundance of security and computer security material available within DOE and Headquarters. There are formal booklets and informal notices.

9.5.1 Training Documents

There is a series of documents issued by DOE and Headquarters to be available to employees and contractors who will access Federal information and use computer systems in their work.

- Computer Incident Advisory Capability Information Bulletins
- Your Responsibilities as DOE Employees, DOE/HR-0145

9.5.2 Notices

DOE Headquarters supports a series of security awareness notices and briefings that promote computer security. Many of these notices are computer-based and some require a user response.

- Computer Incident Advisory Capability (CIAC) Notices.

- Online security notices are published as needed by administrators of mainframe and LAN systems.

- The CPPM disseminates awareness notices.

9.6 Training Records

The CPPM maintains a record of computer security training conducted within each Headquarters organization. The organizational training section maintains individual records of formal computer security training. Additional computer security training records are kept by the ACPPMs as needed to evaluate the security posture of the organization.